REMARKS

In the final office action, Applicant was requested to confirm whether a certified copy of the foreign application has been filed. Claim 12 was objected to because of informalities. Claim 12 was rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,590,199 to Krajewski, Jr. et al. ("Krajewski et al."). Claim 13 was rejected under 35 U.S.C. §103(a) as being unpatentable over Krajewski et al. Claims 1 to 11, 14 and 15 were found to be allowable.

In this response, claim 12 has been amended to correct formalities.

Reconsideration of the application based on the following is respectfully requested

Priority Document

Applicant was requested to confirm whether a certified copy of the foreign application has been filed. A certified copy of priority document EP 99 103 951.2 was filed on March 30, 2004, together with the response to the office action of December 31, 2003. Enclosed with this response applicant submits a copy of form PTO-1083 of said response, a copy of the stamped return receipt postcard and a copy of the cover page of the certified copy of EP 99 103 951.2.

Claim Objections

Claim 12 was objected to because of informalities. Claim 12 has been amended to correct a typographical error and to rewrite the functions in the body of the claim in active form as suggested by the Examiner.

Withdrawal of the objections is respectfully requested.

Response to Arguments

In the "Response to Arguments" section, on page 3 of the final office action, the Examiner provides an explanation for rejecting Applicants previously submitted arguments. Applicants respectfully submit that the Examiner's explanation is flawed for two reasons.

First, the Examiner asserts that the disclosure at column 1, lines 44-46 "implies that Krajewski inherently teaches that a user-id is received from a second computer system and transmitted to said second *computer system*." Thus, even if true, the assertion does not mean that feature a) of claim 12 is taught, since claim 12 requires transmission from the trusted agent to the second security system, and not to the second computer system.

Second, the paragraph relied upon by the Examiner in the Background section of Krajewski et al. is merely a description of the known concept of a "unitary login" (column 1, lines 41-52), and is insufficient for an inherent teaching of feature a) of claim 12. The description of a trusted agent performing a user identification and authentication to each accessed resource "transparently" (i.e. without the user recognizing that it is happening), is not an inherent teaching for the specific feature of a trusted agent receiving a user-id for a second computer system and transmitting it to a second security system. As discussed below, the only unitary login system is described in detail in Krajewski et al., (i.e. the Kerberos system), performs the authentication in a way that is transparent to the user but without performing the function a) of claim 12.

Rejection under 35 U.S.C. §102(b)

Claim 12 was rejected under 35 U.S.C. §102(b) as being anticipated by Krajewski et al. (US 5,590,199).

Krajewski et al. describes an electronic information network user authentication and authorization system. Among several known authentication and authorization systems, the Kerberos protocol is discussed in detail in the Background section. Kerberos utilizes a trusted central authentication server (KAS). The Kerberos system works as follows: A user on a client platform, such as the workstation 14 (see Fig. 3) may intend to access data from a remote location, for example, from a service A connected visa the network 18. In order to control this access, there is an authorization server 32, which is the Kerberos authentication server (KAS). See column 2, lines 20-64.

Independent claim 12 recites a trusted agent for enabling the check of the access of a user operating a first computer system controlled by a first security system to software and/or data on a second computer system controlled by a second security system. The trusted agent performs the following functions:

a) receiving a user-id for said second computer system and transmitting said user-id to said second security system,
b) retrieving a shared secret, which is registered in said fist first security system and in said second security system, from said second security system, and
c) transmitting said shared secret from said trusted agent to said second computer system.

Applicants respectfully that the trusted agent described in Krajewski et al. does not include all of the features of claim 12, and further that the features of claim 12 are not suggested by Krajewski et al.

Specifically, Applicants submit that at least feature a) of claim 12 is not taught or suggested by Krajewski et al. As described in detail at column 2, the Kerberos authentication system issues a ticket in response to a ticket request from a user on a first computer system (e.g. workstation 14). The ticket contains, among other items, the service ID and the user ID. However, the ticket is sent from the KAS back to the user's computer. See column 2, lines 47 to 49, who subsequently transmits the ticket to the service A in order to gain access. There is no suggestion for a communication between KAS and a second security system controlling a second computer system.

Nor is there a suggestion for the feature b) of claim 12. The Kerberos authorization server of Krajewski et al. teaches the use of private keys, as described at column 2, lines 40-42, and each service (corresponding to the second computer system) is a separate entity, each with its own cryptographic key, which may be deemed to be a shared secret. Thus, the shared secrets described in Krajewski et al. are either shared between the first security system and the trusted agent, or shared between the second security system and the trusted agent. There is no secret in Krajewski et al. that is shared between anything on the first computer system (operated by the user) and anything on the server for the service A. On the contrary, it is the centralized KAS which shares all secrets of the Krajewski et al. system. There is likewise no suggestion for the feature of retrieving a shared secret registered in both the first security system and the second security system as recited in claim 12.

Furthermore, the feature c) of claim 12 is likewise not taught or suggested by Krajewski et al. On the contrary, Krajewski et al. teaches the shared secret of service A (i.e. its private key), is used to encrypt the information of the ticket, wherein the ticket is sent from the KAS back to the user on workstation 14. The ticket is then sent from the user (operating the first computer system) to the service A in order to access the data. There is no suggestion for the feature of transmitting the shared secret (received from the second security system) from the trusted agent to the second computer system as recited in claim 12.

Withdrawal of the rejection under 35 U.S.C. §102(b) is respectfully requested.

Rejections under 35 U.S.C. §103(a)

Claim 13 was rejected under 35 U.S.C. §103(a) as being unpatentable over Krajewski et al.

Krajewski discloses a centralized access-control solution, the present invention discloses a non-centralized solution by enabling communication between the first and second security system (see column 2, lines 37 to 41). As explained in detail above, Applicants submit that none of the features a), b), and c) are taught or suggested by Krajewski et al.

Withdrawal of the rejections under 35 U.S.C. §103(a) thus is respectfully requested.

CONCLUSION

The present application is respectfully submitted as being in condition for allowance and applicants respectfully request such action.

Respectfully submitted,
DAVIDSON, DAVIDSON & KAPPEL, LLC

By: ______________________
William C. Gehris, Reg. 38,156
(signing for Thomas P. Canty, Reg. No. 44,586)

DAVIDSON, DAVIDSON & KAPPEL, LLC
Patents, Trademarks and Copyrights
485 Seventh Avenue, 14th Floor
New York, New York 10018
(212) 736-1940